

1 MICHAEL F. RAM (SBN 104805)
2 **MORGAN & MORGAN COMPLEX**
3 **LITIGATION GROUP**

4 633 West Fifth Street, Suite 2652, Los
5 Angeles, CA 90071

6 Telephone: (415) 358-6913

7 Facsimile: (415) 418-6293

8 mram@ForThePeople.com

9 JOHN A. YANCHUNIS
10 (*Pro Hac Vice application forthcoming*)

11 PATRICK A. BARTHLE II
12 (*Pro Hac Vice application forthcoming*)

13 **MORGAN & MORGAN COMPLEX**
14 **LITIGATION GROUP**

15 201 N. Franklin Street, 7th Floor
16 Tampa, Florida 33602

17 Telephone: (813) 559-4908

18 Facsimile: (813) 222-4795

19 jyanchunis@ForThePeople.com

20 pbarthle@ForThePeople.com

21 *Attorneys for Plaintiff and the Proposed Class*

22 **UNITED STATES DISTRICT COURT**

23 **CENTRAL DISTRICT OF CALIFORNIA**

24 WALTER HOPGOOD, individually and on
25 behalf of all other similarly situated,

26 Plaintiff,

27 v.

28 EXPERIAN INFORMATION SOLUTIONS,
INC., a corporation ,

Defendant.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Walter Hopgood, individually and on behalf of all others similarly situated, files this Class Action Complaint against defendant Experian Information Solutions, Inc. (“Experian” or “Defendant”), and in support state the following.

INTRODUCTION

1. Experian is an American–Irish multinational consumer credit reporting company. Experian is a credit reporting agency as that term is defined by the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.* (“FCRA”).¹ Experian collects and aggregates information on over 1 billion people and businesses, including 235 million individual U.S. consumers and more than 25 million U.S. businesses.²

2. As a consumer credit reporting agency, Experian collects and maintains highly detailed sensitive, confidential, and regulated consumer, financial, and personal records and information (“Consumer Data”), including consumer credit information and Social Security numbers (collectively, “PII”) on behalf of Plaintiff and Class Members, much of which is sensitive and not publicly available.

3. Experian mostly collects the information without making any contact with the consumers whose information it sells, and consumers cannot remove their information from Experian’s databases.

4. Experian is one of the “big-three” credit bureaus that maintains information related to the credit history of consumers and sells information to creditors, its business clients, who are considering a borrower’s application for credit or who have extended credit to the borrower. Additionally, Experian also offers credit services that are designed, in theory, to assist customers with managing their credit scores and to monitor for potential acts of fraud.

5. To facilitate this, Experian offers consumers “online access to their credit history and score” by providing the ability to create Experian customer accounts. These accounts grant the account holder with a degree of access to and control over the information Experian has aggregated

¹ See 15 U.S.C. § 1681(f).

² Exhibit 1 (EXPERIAN, *Explaining Experian*), at 2.02

1 about an individual in their Experian credit report.

2 6. This lawsuit arises from Experian's violations of the FCRA that have allowed for a
 3 spate of identity thefts perpetrated using Experian consumer accounts. Plaintiff, along with
 4 similarly situated Class Members, allege that these identity thefts resulted from a combination of
 5 Experian's inadequate security measures and insufficient identity verification procedures related
 6 to Plaintiff's and Class Members' Experian consumer accounts. Plaintiff further alleges that,
 7 because of Experian's insufficient security measures, hackers and cybercriminals can easily and
 8 repeatedly take control of the victims' Experian consumer accounts or create new Experian
 9 accounts in victims' names. The cybercriminals can then use the victims' Experian accounts to
 10 facilitate identity theft (hereinafter the "Security Failure").³

11 7. Defendant's actions or inactions that allowed for the Security Failure also violate
 12 its duties and obligations as a credit reporting agency under the FCRA, as described in detail
 13 herein. Each instance in which Experian has failed to comply with Sections 604 or 607 of the
 14 FCRA, 15 U.S.C. §§ 1681b, 1681e, constitutes a separate violation of the FCRA for the purpose
 15 of assessing monetary damages. Experian's acts described herein constitute a pattern or practice
 16 of knowing violations, as set forth in Section 621(a)(2)(A) of the FCRA, 15 U.S.C. §
 17 1681s(a)(2)(A).

18 8. This action seeks to hold Defendant accountable for its conduct and its repeated
 19 refusal to remedy its security issues and/or deploy additional security measures readily available
 20 to Defendant, such as two-factor or multi-factor authentication. This case seeks vindication and
 21 recompense on behalf of the individual consumers whose Consumer Data and PII was collected,
 22 maintained, and inadequately protected by Experian.

23 9. Plaintiff seeks to recover FCRA statutory damages to the fullest extent allowable
 24 by law. In addition Plaintiff also seeks injunctive relief requiring Defendant to, *inter alia*, (i)

26 ³ According to the United States Government Accounting Office (GAO), the terms "identity
 27 theft" or "identity fraud" are broad terms encompassing various types of criminal activities.
 28 Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include,
inter alia, credit card fraud, phone or utilities fraud, bank fraud and government fraud (filing
 fraudulent tax returns and theft of government services).

1 conduct a full-system audit to finally properly verify the identity of each Experian consumer
 2 account holder using its “robust identity verification services;” (ii) identify and notify each U.S.
 3 citizen whose Experian Consumer Account (a) was accessed and/or claimed by an unauthorized
 4 individual, (b) was otherwise subject to the Security Failure, or (c) was otherwise compromised
 5 by the Security Failure; (iii) provide a sum of money sufficient to provide quality credit monitoring
 6 and substantial identity theft coverage to each such person for each of their respective lifetimes
 7 (iv) establish a fund (in an amount to be determined) to which such persons may apply for
 8 reimbursement of the time and out-of-pocket expenses they incurred to remediate identity theft
 9 and identity fraud (i.e., data breach insurance), from July 27, 2017 forward to the date the above-
 10 referenced credit monitoring terminates, (iv) disgorge its gross revenue from transactions,
 11 including but not limited to the revenue derived from selling Consumer Data to business clients
 12 for applications created by unauthorized individuals involving Plaintiff’s and Class Members’
 13 Consumer Data and PII, and the earnings on such gross revenue, and (vi) discontinue its above-
 14 described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the
 15 causes of the Security Failure.

16 10. Plaintiff and Class Members have standing to sue as a result of Experian’s
 17 violations of federal and state statutes, including the FCRA, as detailed herein. Further, because of
 18 Experian’s acts and/or omissions, willful disregard and conduct, and want of ordinary care, and
 19 the resulting Security Failure, Plaintiff and Class Members have suffered actual injury have
 20 suffered (and will continue to suffer) economic damages and other injury and actual harm in the
 21 form of, *inter alia*, (i) actual identity theft and identity fraud, causing immense damage to each
 22 individual’s credit score, (ii) invasion of privacy, (iii) loss of the intrinsic value of their privacy,
 23 (iv) breach of the confidentiality of their Consumer Data and PII, (v) deprivation of the value of
 24 their Consumer Data and PII, for which there is a well-established national and international
 25 market, (vi) the financial and temporal cost of monitoring their credit, monitoring their financial
 26 accounts, and mitigating their damages, and (vii) the imminent, immediate, and continuing
 27 increased risk of ongoing identity theft and identity fraud. Plaintiff also have standing to bring this
 28 suit because Defendant has yet to remedy the cause of the Security Failure.

THE PARTIES

11. Plaintiff and Class Members are individuals whose Consumer Data and PII is contained within Experian's database and have or had an Experian consumer account associated with their Consumer Data and PII.. Plaintiff brings claims on behalf of other similarly-situated individuals with Experian consumer accounts residing in in the United States (the "Class" defined in Paragraph 141, hereinafter the members of the Class are referred to as "Class Members") arising from Experian's Security Failure.

12. Plaintiff Walter Hopgood ("Hopgood") is an adult domiciled in Clackamas County, Oregon. Hopgood has an active Experian account. Plaintiff Hopgood's Experian CreditWorks Basic consumer account ("Experian consumer account") and the information therein was repeatedly accessed and stolen by an unauthorized cybercriminal, resulting in his identity being stolen, inaccurate information being placed onto his credit report, his credit report being furnished for impermissible purposes, and dozens of attempts to open fraudulent accounts in his name.

13. Defendant Experian Information Solutions, Inc. is a privately held company that maintains its North American headquarters in Costa Mesa, California. Experian is authorized to do business throughout the country and in the State of California. Experian is a "consumer reporting agency" as defined in 15 U.S.C. § 1681a(f).

14. Experian transacts or has transacted business in this District and throughout the United States. At all times material to this Complaint, Experian has operated a business through its website, its consumer and business portals, and through its mobile applications.

JURISDICTION AND VENUE

15. This Court has personal jurisdiction over Defendant because Experian's principal place of business is in California. Additionally, Defendant is subject to specific personal jurisdiction in this State because a substantial part of the events and conduct giving rise to Plaintiff's and Class Members' claims occurred in this State, including Experian servers in California executing the fraudulent operations and maintaining the data at issue, and because of how employees of Experian in California reuse the communications and data collected.

16. This Court has subject matter jurisdiction over this entire action pursuant to the

1 Class Action Fairness Act (“CAFA”), 28 U.S.C. § 1332(d), because this is a class action in which
 2 the amount in controversy exceeds \$5,000,000, and at least one Class member is a citizen of a
 3 state other than California. Further, this Court has federal question jurisdiction over this entire
 4 action pursuant to 15 U.S.C. § 1681p, which grants jurisdiction to any appropriate United States
 5 District Court, without regard to the amount in controversy.

6 17. Venue is proper in this District because a substantial portion of the events and
 7 actions giving rise to the claims in this matter took place in this judicial District. Furthermore,
 8 Experian is headquartered in this District and subject to personal jurisdiction in this District.

9 **FACTUAL ALLEGATIONS**

10 **I. Consumer Reporting Agencies and the Fair Credit Reporting Act’s Requirements**

11 18. Consumer reporting agencies assemble and evaluate credit, public record, and other
 12 consumer information into consumer reports or “credit reports.”⁴

13 19. The information in these reports is used by many different types of businesses,
 14 from creditors and insurers to landlords and employers, to make eligibility and other decisions
 15 about consumers.⁵ Creditors, for example, use information in consumer reports to determine
 16 whether, and on what terms, to extend credit to a particular consumer or at what interest rate credit
 17 should be extended to that consumer.

18 20. According to the Consumer Financial Protection Bureau (“CFPB”), “[t]his
 19 collection, assembly, evaluation, dissemination, and use of vast quantities of often highly
 20 sensitive personal and financial information [by consumer reporting agencies] about consumers
 21 poses significant risks to consumer privacy.”⁶

22 21. Accuracy and confidentiality in consumer reports is of vital importance to the
 23 consumer reporting system, particularly as consumer reports play an increasingly important role
 24

25 ⁴ See 15 U.S.C. 1681a(d) (defining “consumer report”).

26 ⁵ Bureau of Consumer Fin. Prot., *Fair Credit Reporting; Permissible Purposes for Furnishing,*
 27 *Using, and Obtaining Consumer Reports*, Advisory Opinion (Jul. 7, 2022), available at:
 28 [https://files.consumerfinance.gov/f/documents/cfpb_fair-credit-reporting_advisory-](https://files.consumerfinance.gov/f/documents/cfpb_fair-credit-reporting_advisory-opinion_2022-07.pdf)
[opinion_2022-07.pdf](https://files.consumerfinance.gov/f/documents/cfpb_fair-credit-reporting_advisory-opinion_2022-07.pdf) (last visited Jul. 24, 2022) (hereinafter “*Fair Credit Reporting 2022*
Advisory Opinion”).

⁶ *Fair Credit Reporting 2022 Advisory Opinion*, at 2.

1 in the lives of American consumers.⁷

2 22. Accordingly, among other policy goals, Congress enacted the Fair Credit Reporting
3 Act, 15 U.S.C. § 1681, *et seq.* (“FCRA”) “to ensure fair and accurate credit reporting, promote
4 efficiency in the banking system, and protect consumer privacy.”⁸

5 23. Among other things, the FCRA “require[s] that consumer reporting agencies adopt
6 reasonable procedures for meeting the needs of commerce for consumer credit, personnel,
7 insurance, and other information in a manner which is fair and equitable to the consumer, with
8 regard to the confidentiality, accuracy, relevancy, and proper utilization of such information.” 15
9 U.S.C.A. § 1681(b),

10 24. The CFPB recently emphasized the importance of confidentiality of consumer credit
11 reports in its *Fair Credit Reporting 2022 Advisory Opinion*:

12 Consumers suffer harm when consumer reporting agencies provide
13 consumer reports to persons who are not authorized to receive the
14 information or when recipients of consumer reports obtain or use
15 such reports for purposes other than permissible purposes. These
16 harms include the invasion of consumers’ privacy, as well as
17 reputational, emotional, physical, and economic harms.⁹

18 25. Accordingly, the FCRA places obligations on credit reporting agencies when it
19 comes to the security, accuracy, and confidentiality of consumer credit reports. The FCRA
20 protects consumer privacy in multiple ways, including by limiting the circumstances under which
21 consumer reporting agencies may disclose consumer information.

22 26. For example, FCRA section 604, entitled “Permissible purposes of consumer
23 reports,” identifies an exclusive list of “permissible purposes” for which consumer reporting
24 agencies may provide consumer reports.¹⁰

25 27. The statute clearly states that “a consumer reporting agency shall not furnish to any

26 ⁷ See 15 U.S.C. 1681-1681x.

27 ⁸ *Safeco Ins. Co. of Am. v. Barr*, 551 U.S. 47, 52 (2007); *see also* 15 U.S.C. 1681 (recognizing “a
28 need to insure that consumer reporting agencies exercise their grave responsibilities with
fairness, impartiality, and a respect for the consumer’s right to privacy”).

⁹Bureau of Consumer Fin. Prot., *Fair Credit Reporting; Name-Only Matching Procedures*, 86 FR
62468, 62472 (Nov. 10, 2021), *available at*
[https://files.consumerfinance.gov/f/documents/cfpb_fair-credit-reporting_advisory-
opinion_2022-07.pdf](https://files.consumerfinance.gov/f/documents/cfpb_fair-credit-reporting_advisory-opinion_2022-07.pdf).

¹⁰ See 15 U.S.C. 1681b(a) (providing that, “[s]ubject to subsection (c), any consumer reporting
agency may furnish a consumer report under the following circumstances and no other”).

1 person a record of inquiries in connection with a credit or insurance transaction that is not initiated
 2 by the consumer” unless the consumer has given authorization to the consumer reporting agency.
 3 15 U.S.C. 1681b(c)(3).

4 28. Section 607(b) of the FCRA, 15 U.S.C. § 1681e(b), requires that “[w]henver a
 5 consumer reporting agency prepares a consumer report it shall follow reasonable procedures to
 6 assure maximum possible accuracy of the information concerning the individual about whom the
 7 report relates.”

8 29. This includes maximum possible accuracy with respect to the information that is
 9 included on an individual’s credit report – including, but not limited to the number of applications
 10 for credit that individual has filed.¹¹

11 30. The Bureau has recently affirmed that, “[i]n preparing consumer reports, it is not a
 12 reasonable procedure to assure maximum possible accuracy” if a consumer reporting agency uses
 13 “insufficient identifiers to match information to the consumer who is the subject of the report.”¹²

14 31. Further, consumer reporting agencies are prohibited from furnishing credit reports if
 15 they suspect that it is not for a purpose explicitly listed in Section 604. 15 U.S.C. § 1681e(a).

16 **II. Experian Willfully Violates its Obligations as a Consumer Reporting Agency**

17 32. Experian is a national consumer reporting agency as defined in the FCRA. 15
 18 U.S.C. § 1681a(f).

19 33. According to Defendant, “Experian’s goal as a consumer credit reporting agency is
 20 to help lenders make better informed lending decisions and to make it quicker and easier for
 21 consumers to obtain finance.”¹³

22 34. Experian collects massive amounts of information on people, businesses, motor
 23 vehicles, insurance, and lifestyle data, including data pertaining to United States citizens and
 24 residents. Experian mostly collects the information without making any contact with the
 25

26 ¹¹ Consumer Fin. Prot. Bur., *Fair Credit Reporting: Permissible Purposes for Furnishing and*
 27 *Using and Obtaining Consumer Reports*, 87 FR 41243 (Jul. 7, 2022), available at
 28 <https://www.federalregister.gov/d/2022-14823/p-41>.

¹² *Id.*

¹³ Exhibit 1 (EXPERIAN, *Explaining Experian* (May 2007))(emphasis added), at 2.02

1 consumers whose information it sells, and consumers cannot remove their information from
2 Experian's databases.

3 35. For over four decades "Experian has developed core expertise in acquiring,
4 processing and managing operating very large and comprehensive databases" and maintains "very
5 detailed historical information" on over 215 million adult consumers in the United States.¹⁴

6 36. Experian states that its United States credit database is "ranked by industry analysts
7 as one of the largest databases in the world and includes over 10 billion lines of data."

8 37. Using this data, Experian derives revenue streams from consumers in two ways: (1)
9 directly from the consumer (in the form of identity monitoring, insurance, and fraud restoration
10 services); (2) indirectly by selling access to consumers' information to businesses and
11 government organizations, among other business-to-business services including, notably, a
12 claimed expertise in fraud detection and identity verification.¹⁵

13 38. Companies with numerous revenue streams derived from collecting vast amounts
14 of Consumer Data and PII, like Experian, recognize the monetary value of consumers' personal
15 information and the value of having sole control over the most amount of data. About its business
16 model, Experian states:

17 At the core of Experian are comprehensive databases of credit and
18 marketing information on consumers and businesses. These
19 databases are derived from both public and private sources and
20 contain extensive, high quality information with considerable
21 historical depth. Our comprehensive portfolio of data is maintained
22 and owned by Experian and ***offers a greater breadth of information***
23 ***than any single competitor***, making us a partner of choice to many
24 clients.¹⁶

25 39. Thus, Experian seeks to collect, aggregate, maintain, and analyze data about
26 consumers from public and nonpublic sources explicitly for the purpose of selling that
27
28

29 ¹⁴ *Id.*

¹⁵ Experian's principal lines of business are credit services, marketing services, decision
analytics, and consumer services. *Id.*

¹⁶ *Id.*

information to businesses (Defendant’s “clients”), in exchange for monetary benefits.¹⁷

a. Experian Sells Credit Services Directly to Consumers

40. Experian is one of the “big-three” credit bureaus that offer credit services that are designed, in theory, to assist customers with managing their credit scores and to monitor for potential acts of fraud.

41. To facilitate this, Experian offers consumers the ability to create accounts that provide the account holder with a degree of access to and control over the information Experian has aggregated about an individual in their Experian credit report, including the credit report itself and the ability to freeze or unfreeze (or lock and unlock) that individual’s Experian credit report.

42. An account holder’s control over the associated Experian credit report varies with the amount of money the account holder pays to Experian – with the Experian CreditWorks basic consumer account that can be opened free of charge, individuals can lock parts of their credit report from being accessed by would-be creditors.

43. For an additional monthly payment, consumers can pay for identity monitoring services, security freezes, and, allegedly, extra credit report security.

44. Experian also sells services to assist consumers with identity theft restoration following instances of identity theft.

45. Experian encourages consumers to provide as much information to Experian as possible, including offering services such as ExperianBoost, which connects consumers’ utility and rent payments to Experian’s database in exchange for a purported credit boost.

b. Experian Sells Consumer Data to Businesses

46. On the other side of the coin, Experian generates and sells credit reports containing consumer information and details of a consumer’s credit history to businesses and its recurring

¹⁷ Kari Paul, *Google launches app that will pay users for their data*, The Guardian (June 11, 2019), <https://www.theguardian.com/technology/2019/jun/11/facebook-user-data-app-privacy-study>; Saheli Roy Choudhury and Ryan Browne, *Facebook pays teens to install an app that could collect all kinds of data*, CNBC (Jan. 30, 2019), <https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html>; Jay Peters, *Facebook will now pay you for your voice recordings*, The Verge (Feb. 20, 2020), <https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-pronunciations-app>.

1 clients.

2 47. Credit reports are used by parties to determine whether and on what terms a
3 consumer will be offered credit, including credit cards, student, car, and small business loans,
4 mortgages, rental housing, and insurance.

5 48. According to Experian, “when a consumer applies for credit, lenders usually contact
6 a credit reporting agency for a consumer credit reference check to confirm the person’s identity
7 and creditworthiness.”¹⁸

8 49. Each time an individual’s credit report is requested from a consumer reporting
9 agency or by a potential creditor, that hard inquiry is noted on the consumer’s credit report. Hard
10 inquiries are considered to be negative items on a consumer’s credit report. An application for a
11 line of credit, such as a credit card, debit card, or consumer spending account, can cause a “hard
12 inquiry” to appear on a consumer’s credit report. These credit entries are among the information
13 that consumer reporting entities are obligated to ensure remain accurate and confidential.

14 50. Notably, for business clients, “Experian offers a range of fraud prevention tools
15 which are used by hundreds of the world’s leading financial institutions” to achieve “greater fraud
16 prevention success.”¹⁹

17 51. Defendant states that its “[a]uthentication services provide the information needed
18 to instantly verify customer identity and prevent fraud, while conducting secure transactions
19 online and at call centres.”²⁰

20 ***c. The Security Failure and Experian’s Account Security Insufficiencies***

21 52. In July of 2022, reports about the Security Failure began to surface, detailing the
22 stories of consumers whose Experian consumer accounts had been hacked and updated with a new
23 email address belonging to an unauthorized cybercriminal.

24 53. Early reporting suggested that identity thieves were able to hijack Experian
25 consumer accounts simply by signing up for new accounts at Experian using the victim’s personal
26

27 ¹⁸ *Id.*

28 ¹⁹ Ex. 1.

²⁰ Ex. 1.

1 information and a different email address.

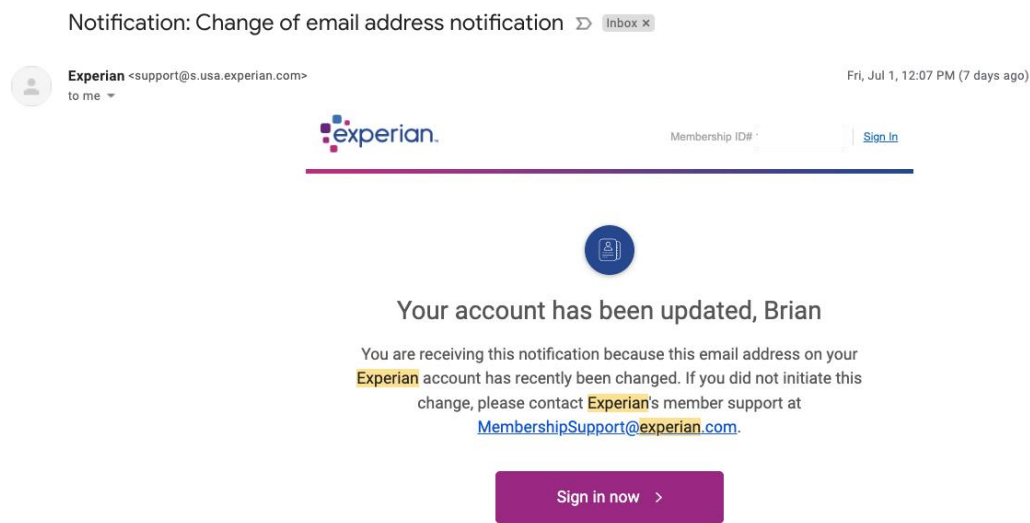
2 54. According to reporting by KREBSONSECURITY, the Security Failure allows new
3 Experian consumer accounts to override the control of existing consumer accounts, even in cases
4 where consumers used password managers to select strong, unique passwords for their Experian
5 consumer accounts.

6 55. Without using any advanced technological maneuvers, cybercriminals are able to
7 steal access to any Experian consumer account using that consumer's name, date of birth, and Social
8 Security number, in combination with information readily available in public records.

9 56. At that point, the account password can be set by the cybercriminal, and subsequent
10 requests to reset the password by the real owner to take back control will be sent to an email address
11 the victims do not have access to.

12 57. Subsequent reporting and discussions on threads dedicated to data privacy and
13 cybersecurity reveal that Security Failure allows cybercriminals to obtain control over Experian
14 consumer accounts – regardless of whether an individual has an existing consumer account with
15 Experian.

16 58. If the victim has an existing Experian account, the victim could potentially be alerted
17 of the loss of access to their account with an email from Experian, like the one pictured below,
18 stating that their account information had been changed:



28 59. However, if the victim has not set up an account with an email address where

1 Experian can alert them of the new email, the victim will remain unaware that their Experian
2 account has been claimed by an unauthorized cybercriminal.

3 60. Reporting by KREBSONSECURITY was able to easily replicate the effects of the
4 Security Failure. In his July 11, 2022 article, Brian Krebs successfully sought to recreate his
5 Experian consumer account using a different email address; he wrote, in part:

6 [The investigation sought to determine whether] Experian would
7 allow me to re-create my account using my personal information
8 but a different email address. The experiment was done from a
different computer and Internet address than the one that created
the original account years ago.

9 After providing my Social Security Number (SSN), date of birth,
10 and answering several multiple choice questions whose answers
11 are derived almost entirely from public records, Experian promptly
12 changed the email address associated with my credit file. It did so
without first confirming that new email address could respond to
messages, or that the previous email address approved the change.

13 Experian's system then sent an automated message to the original
14 email address on file, saying the account's email address had been
15 changed. The only recourse Experian offered in the alert was to
sign in, or send an email to an Experian inbox that replies with the
message, "this email address is no longer monitored."²¹

16 61. After successfully taking control of his account from a new, unverified computer,
17 KREBSONSECURITY reported:

18 Experian [then] prompted me to select new secret questions and
19 answers, as well as a new account PIN — effectively erasing the
20 account's previously chosen PIN and recovery questions. Once I'd
21 changed the PIN and security questions, Experian's site helpfully
reminded me that I have a security freeze on file, and would I like
to remove or temporarily lift the security freeze?

22 To be clear, Experian does have a business unit that sells one-time
23 password services to businesses. While Experian's system did ask
24 for a mobile number when I signed up a second time, at no time
25 did that number receive a notification from Experian. **Also, I could
26 see no option in my account to enable multi-factor
authentication for all logins.**²²

27 ²¹ KREBSONSECURITY, *Experian, You Have Some Explaining To Do*, KREBSONSECURITY (Jul.
28 11, 2022), available at <https://krebsonsecurity.com/2022/07/experian-you-have-some-explaining-to-do/> (last visited Jul. 25, 2022).

²² *Id.* (emphasis added).

62. Importantly, the reporting also noted that similar techniques failed to steal accounts from Equifax and TransUnion “the other two big consumer credit reporting bureaus.”²³ The reporting continued:

When KrebsOnSecurity tried to re-create an existing account at TransUnion using my Social Security number, TransUnion rejected the application, noting that I already had an account and prompting me to proceed through its lost password flow. The company also appears to send an email to the address on file asking to validate account changes.

Likewise, trying to recreate an existing account at Equifax using personal information tied to my existing account prompts Equifax’s systems to report that I already have an account, and to use their password reset process (which involves sending a verification email to the address on file).²⁴

63. In a written statement, Experian suggested public reporting about the Security Failure were aberrations, and “that its security and identity verification practices extend beyond what is visible to the user” according to the article.²⁵

64. “We believe these are isolated incidents of fraud using stolen consumer information,” Experian’s statement reads.²⁶

65. Experian states “[O]nce an Experian account is created, if someone attempts to create a second Experian account, our systems will notify the original email on file.”²⁷

66. Experian’s statement to KREBSONSECURITY continues:

“We go beyond reliance on personally identifiable information (PII) or a consumer’s ability to answer knowledge-based authentication questions to access our systems [. . .]

We do not disclose additional processes for obvious security reasons; however, our data and analytical capabilities verify identity elements across multiple data sources and are not visible to the consumer. This is designed to create a more positive experience for our consumers and to provide additional layers of protection. We take consumer privacy and security seriously, and we continually review our security processes to guard against constant and evolving

²³ *Id.*

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Id.*

²⁷ *Id.*

threats posed by fraudsters.”

67. Despite Experian’s statements, experts maintain that Experian’s identity verification measures are insufficient. For example, Emory Roan, policy counsel for the Privacy Rights Clearinghouse, said “Experian not offering multi-factor authentication for consumer accounts is inexcusable in 2022.” Roan further stated:

[Experian] compound[s] the problem by gating the recovery process with information that’s likely available or inferable from third party data brokers, or that could have been exposed in previous data breaches,” Roan said. ‘Experian is one of the largest Consumer Reporting Agencies in the country, trusted as one of the few essential players in a credit system Americans are forced to be part of. For them to not offer consumers some form of (free) MFA is baffling and reflects extremely poorly on Experian.’²⁸

68. Indeed, even after Experian is alerted that an Experian consumer account has been hacked or that there has been attempted identity theft on an individual with an Experian consumer account, Experian does not add additional identity verification procedures.

69. Upon information and belief, even after Experian receives information *directly from the consumer* that indicates that the consumer is a victim of identity theft and that the victim’s account is compromised, Experian adds no additional identity verification procedures that prevent the hacker from regaining control over the account.

70. Upon information and belief, even after receiving reports that an individual’s Experian consumer account has been hacked, Experian continues to sell and/or furnish that victim’s Experian credit report to businesses that request that victim’s credit report. Experian continues to provide these reports even if the business’ request is clearly in response to a fraudulent application filed in that individual’s name.

71. Upon information and belief, even after being notified that an individual’s Experian credit report has been hacked, Experian will continue to furnish that individual’s credit report in response to fraudulent applications and will even inaccurately include those fraudulent applications as hard inquiries on that victim’s Experian credit report.

²⁸ *Id.*

d. ***Experian Provides Insufficient Identity Verification Procedures While Offering “Robust” Services to Businesses***

72. Experian’s identity verification procedures intended to protect Experian consumers accounts have long been criticized by cybersecurity experts and policymakers.²⁹ Notably, Experian has a self-described “robust” selection of Fraud Prevention services it offers to its business clients, yet the verification procedures used to protect consumers fall short of industry standards and regulatory requirements.

73. Experian touts its ability to “help businesses recognize true identities to establish trusted relationships with legitimate customers while keeping fraudsters out.”³⁰

74. Indeed, Experian offers business clients “robust verification options” to recognize true consumer identities; it states that it can provide “[e]ver-evolving solutions to manage identity verification with confidence even for identities that may have previously been compromised” to ***businesses***.³¹

75. However, despite its robust identity verification offerings for its paying business customers, upon information and belief, Experian fails to implement these robust consumer identity verification offerings to its base of Experian consumer account holders.

76. Upon information and belief, the only piece of non-public information used to verify an identity when signing up for a free Experian consumer account is an individual’s Social Security number. All other pieces of information, such as name, date of birth, and the answers to the “knowledge based” authentication questions (“KBAs”) can readily be found using basic search engines.

77. Thus, once a cybercriminal acquires a Social Security number from any source, such as the dark web, that individual can easily claim that individual’s Experian consumer account.

²⁹ KREBSONSECURITY, *Experian’s Credit Freeze is Still A Joke* (Apr. 2021), available at <https://krebsonsecurity.com/2021/04/experians-credit-freeze-security-is-still-a-joke/>;

KREBSONSECURITY, *Experian API Exposed the Credit Scores of Most Americans*, KREBSONSECURITY (Apr. 2021), available at <https://krebsonsecurity.com/2021/04/experian-api-exposed-credit-scores-of-most-americans/>.

³⁰ <https://www.experian.com/business/solutions/fraud-management?rdr=b2b-refresh>

³¹ <https://www.experian.com/business/solutions/fraud-management?rdr=b2b-refresh>

1 78. Nicholas Weaver, a researcher for the International Computer Science
 2 Institute at University of California, Berkeley, said Experian has no real incentive to do things
 3 right on the consumer side of its business. That is, he said, unless Experian’s customers — banks
 4 and other lenders — choose to vote with their feet because too many people with frozen credit
 5 files are having to deal with unauthorized applications for new credit. Weaver continued:

6 The actual customers of the credit service don’t realize how much
 7 worse Experian is, and this isn’t the first time Experian has screwed
 8 up horribly [. . .] Experian is part of a triopoly, and I’m sure this is
 9 costing their actual customers money, because if you have a credit
 freeze that gets lifted and somebody loans against it, it’s the lender
 who eats that fraud cost.³²

10 79. Weaver noted that lenders, unlike consumers, have a choice in which of the triopoly
 11 handles their credit checks and added “I do think it’s important to point out that their real
 12 customers do have a choice, and they should switch to TransUnion and Equifax.”³³

13 80. Plaintiff and Class Members would not have engaged with Experian, nor allowed
 14 Experian to monetize their “highly detailed” and sensitive Consumer Data and PII had Plaintiff
 15 and Class Members been fully informed about the Security Failure and Experian’s insufficient
 16 security measures.

17 81. Defendant was informed, through its agents and directly by Plaintiff, on numerous
 18 occasions about the Security Failure, yet failed to implement a more stringent procedure for
 19 identity verification for Experian consumer accounts. Defendant’s conduct fails to meet industry
 20 standards and continued for years, though Defendant had numerous available means or methods
 21 through which it could freely bring its identity verification procedures in line with its peer credit
 22 reporting agencies.

23 82. Experian refused to correct the Security Failure and subsequently profited off of
 24 the Security Failure by continuing to sell credit reports to business clients, even when Experian
 25 *knew* that accounts had been compromised by identity thieves. Experian’s acts described herein

27 ³² KREBSONSECURITY, *Experian, You Have Some Explaining To Do*, KREBSONSECURITY (Jul.
 28 11, 2022), available at <https://krebsonsecurity.com/2022/07/experian-you-have-some-explaining-to-do/> (last visited Jul. 25, 2022).

³³ *Id.*

1 constitute a pattern or practice of willful and knowing FCRA violations, as set forth in Section
2 621(a)(2)(A) of the FCRA, 15 U.S.C. § 1681s(a)(2)(A).

3 **III. Experian's Consumer Privacy Policies and the Security Failure**

4 83. Experian's Privacy Policy states: "We use a variety of security systems to safeguard
5 the information we maintain and provide We maintain physical security for our facilities and
6 limit access to critical areas We conduct approval processes before information Experian
7 maintains can be accessed or changed."³⁴

8 84. In its consumer privacy policy, Experian promises to "comply with all laws and
9 applicable self-regulatory guidelines."³⁵ Further, Experian's Consumer Privacy Policy states, in
10 part:

11 **How We Secure Your Personal Information**

12 We have appropriate physical, technical, and organizational
13 measures, and tools in place to protect your personal information
14 against the loss, misuse, and alteration of information that complies
15 with relevant legal requirements and best practices. When you enter
16 sensitive information (such as a credit card, Social Security number,
17 or login credentials) into the Site, we encrypt the transmission of
18 that information using Secure Socket Layer (SSL) technology.

19 When you provide information through the Site, you should be
20 aware that your information may be transmitted across the Internet,
21 and no method of transmission over the Internet is 100% secure.
22 Although we take reasonable security measures to protect your
23 information when we receive it, you also need to ensure you take
24 appropriate steps to protect your information. If you have reason to
25 believe that your interaction with us is no longer secure (for
26 example, if you feel that the security of any account you might have
27 with us has been compromised), please notify us of the problem as
28 soon as possible by contacting us.³⁶

22 85. Experian states that it "considers itself a steward of the information it collects,
23 maintains and utilizes. Our responsibility is to ensure the security of the information in our care and
24 to maintain the privacy of consumers through appropriate, responsible use."³⁷

25 86. Experian has dozens of "Information Policies" (found at

27 ³⁴ https://www.experian.com/privacy/information_values (last visited July 25, 2022).

28 ³⁵ *Id.*

³⁶ Exhibit 2 (Privacy Policy).

³⁷ <https://www.experian.com/privacy/>

1 <https://www.experian.com/privacy/>). The policies vary to meet the legal requirements and
 2 consumer expectations in the area in which the information product or service is being used.
 3 Experian states that each of its information policies are built on its “Global Information Values,”
 4 more specifically define how information may be used.³⁸

5 87. Experian states “[u]nderlying [each of] these policies is Experian’s commitment to
 6 provide consumers notice, choice and education about the use of personal information. Educated
 7 consumers are better equipped to be effective, successful participants in a world that increasingly
 8 relies on the exchange of information to efficiently deliver the products and services consumers
 9 demand.”³⁹

10 88. Experian’s “Global Information Values”—attached hereto as **Exhibit 3**, and as set
 11 out at https://www.experian.com/privacy/global_information — state, in part:

12 In the United States, Experian does the following to uphold its
 13 Global Information Values:

14 [. . .]

15 **Accuracy**

- 16 • We acquire information from reputable sources and take
 17 reasonable precautions to ensure and maintain the accuracy of
 18 that information
- 19 • We employ quality control procedures that help identify
 20 inaccurate or out-of-date information and minimize the addition
 21 of such information to our databases
- 22 • We periodically audit the information within our databases to
 23 maximize its accuracy and currentness
- 24 • *Before we provide information to a client, we understand how
 25 that information is going to be used and we ensure that its use
 26 will be fair to consumers*
- 27 • We frequently update the information in our databases to ensure
 28 it is as current as possible

29 [. . .]

- 30 • We provide a process for consumers to dispute information
 31 within their credit report that they believe is inaccurate

32 **Security**

33 *We use a variety of security systems to safeguard the
 34 information we maintain and provide*

35 ³⁸ *Id.*

36 ³⁹ <https://www.experian.com/privacy/>

We maintain physical security for our facilities and limit access to critical areas

We conduct approval processes before information Experian maintains can be accessed or changed

Integrity

We comply with all laws and applicable self-regulatory guidelines

We respond to marketplace signals that our use of information has gone beyond reasonable public expectations and make appropriate changes to meet marketplace needs while remaining within those expectations

We acquire information with assurance that it has been obtained legally and can be provided to us for use and disclosure

We comply with all contractual restrictions placed on information provided to Experian

[. . .]

Communication

We are open and honest about the types of information we maintain, our information sources and how the information is used

We maintain a dialogue with consumer advocates, clients, consumers, government officials and industry associations about privacy concerns

We educate consumers, clients and employees about our business and our Information Values

We actively encourage clients to comply with applicable self-regulatory practices

On our Web site, we give clear notice regarding the information we collect, how the information will be used and what choices consumers have regarding such use.⁴⁰

IV. Experian's Repeated Consumer Privacy Violations

89. The exact type of insufficient security measures at issue in this case have been repeatedly brought to Experian's attention but have been ignored, leaving consumers at the mercy of identity thieves.⁴¹ Experian has, instead, repeatedly chosen to prioritize profit over consumer privacy. Experian's profit-making pursuit has put the privacy and confidentiality of consumers'

⁴⁰ Exhibit 3 (Experian's Global Information Values).

⁴¹ See, e.g., KREBSONSECURITY, *Experian Site Can Give Anyone Your Credit Freeze PIN* (Sept. 2017), available at <https://krebsonsecurity.com/2017/09/experian-site-can-give-anyone-your-credit-freeze-pin/> (last visited Jul. 27, 2022).

1 Consumer Data and PII at risk on more than one occasion.

2 90. Indeed, Experian's insufficient regulatory compliance procedures and insufficient
3 security measures have violated consumers' privacy rights on numerous well-publicized
4 occasions over the past decade.

5 91. For example, in 2013, Experian directly sold access to over 200 million
6 individuals' Consumer Data, including PII, to an online identity theft service.⁴²

7 92. Additionally, on October 1, 2015, Experian announced that it had discovered a
8 data breach existing between September 1, 2015 and September 16, 2015.⁴³ As many as 15 million
9 people who used the company's services, among them customers of American cellular company
10 T-Mobile who had applied for Experian credit checks, may have had their private information
11 exposed.⁴⁴

12 93. On October 31, 2020, public reporting emerged that Experian had suffered another
13 breach, and, though Experian initially claimed the incident had been contained, the breach
14 allegedly exposed the private personal information of over 24 million South African citizens and
15 nearly 800,000 businesses.⁴⁵

16 94. Next, In January 2021, Experian's Brazilian subsidiary allegedly suffered a breach
17 that caused the dark web sale of the private information of 220 million individuals, amounting to
18 nearly every single adult in Brazil.⁴⁶

19 95. Despite the numerous privacy and information security failures allegedly
20

21 ⁴² KREBSONSECURITY, *Experian Sold Consumers Data to ID Theft Service*, available at
22 <https://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service/> (last
visited Jul. 27, 2022).

23 ⁴³ Thielman, Sam, *Experian hack exposes 15 million people's personal information*, THE
GUARDIAN (Oct 2, 2015).

24 ⁴⁴ *Experian Breach Affects 15 Million Consumers*, KREBS ON SECURITY (Sept. 16, 2017).

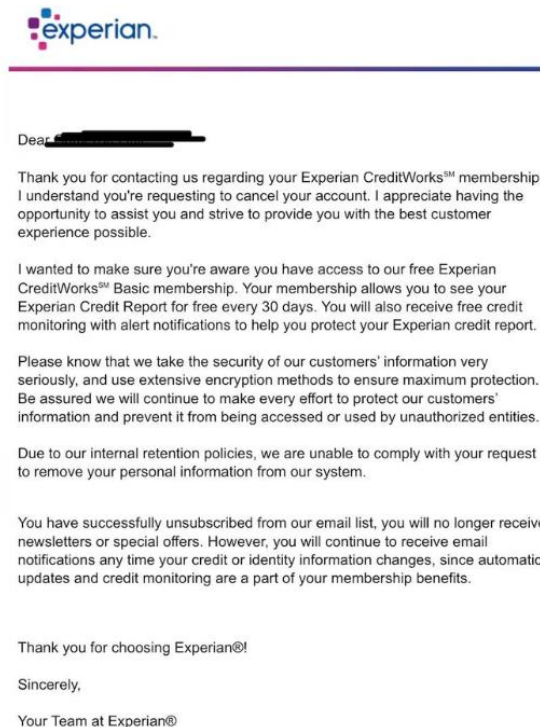
25 ⁴⁵ *Experian Data Breach*, SABRIC (Oct. 31, 2020), available at [https://www.sabric.co.za/media-](https://www.sabric.co.za/media-and-news/press-releases/experian-data-breach)
and-news/press-releases/experian-data-breach; Shange, Naledi, *How Experian was duped into*
26 *handing over data on 24 million South Africans*, TIMESLIVE SOUTH AFRICA (Aug. 20, 2020),
available at [https://www.timeslive.co.za/news/south-africa/2020-08-20-how-experian-was-](https://www.timeslive.co.za/news/south-africa/2020-08-20-how-experian-was-duped-into-handing-over-data-on-24-million-south-africans)
duped-into-handing-over-data-on-24-million-south-africans.

27 ⁴⁶ *The largest personal data leakage in Brazilian history*, OPENDEMOCRACY.NET (FEB. 21, 2021),
28 available at <https://www.opendemocracy.net/en/largest-personal-data-leakage-brazilian-history>.

1 attributable to Experian, the company provides consumers with no recourse.

2 96. Upon information and belief, customers seeking to delete their member accounts
3 may not remove their personal information from Experian's systems due to "internal retention
4 policies."

5 97. For example, one online commenter requested that Experian remove his
6 information from their system and delete his account, and allegedly received the response
7 screenshotted below:



18 47

21 98. As explained above, Experian offers its business clients the option to subscribe or
22 purchase services that allows business to screen for fraudulent applications for accounts or credit
23 lines.

24 99. At the same time, Experian enables the fraud its customers pay to prevent and detect
25 by providing hackers access to Experian accounts, even those it knows to be compromised, as
26

27 ⁴⁷ REDDIT, Thread, Comment
28 https://www.reddit.com/r/assholedesign/comments/vi199w/experian_you_may_not_stop_all_emails_from_us_you/?utm_source=share&utm_medium=ios_app&utm_name=iossmf (last visited July 25, 2022)

1 alleged in this Complaint.

2 100. Experian's practices are willful violations of numerous requirements placed upon
3 Experian by the Fair Credit Reporting Act, are violative of numerous state privacy and consumer
4 protection statutes, and have unjustly enriched Experian at the expense of the millions of American
5 consumers whose data Experian collects and maintains without adequate safeguards.

6
7 **V. Tolling of the Statute of Limitations**

8 101. The preceding factual statements and allegations are incorporated by reference

9 102. Any applicable statutes of limitations have been tolled under (1) the fraudulent
10 concealment doctrine, based on Experian's knowing and active concealment and denial of the facts
11 alleged herein and (2) the delayed discovery doctrine, as Plaintiff did not and could not reasonably
12 have discovered Experian's conduct alleged herein until shortly before the Complaint was filed.

13 103. Experian never disclosed, or adequately disclosed, the existence of the Security
14 Failure and continues to deny its existence.

15 104. **FRAUDULENT CONCEALMENT.** Defendant took active steps to conceal its above-
16 described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the
17 resulting Security Failure and FCRA violations. The details of Defendant's efforts to conceal its
18 above-described unlawful conduct are in its possession, custody, and control, to the exclusion of
19 Plaintiff, and await further discovery. When this material information was first revealed to Plaintiff,
20 they exercised due diligence by investigating the situation, retaining counsel, and pursuing their
21 claims. Defendant fraudulently concealed its above-described wrongful conduct. Should such be
22 necessary, therefore, all applicable statutes of limitation (if any) are tolled under the fraudulent
23 concealment doctrine.

24 105. **EQUITABLE ESTOPPEL.** Defendant took active steps to conceal its above-described
25 wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the resulting
26 Security Failure and FCRA violations. The details of Defendant's efforts to conceal its above-
27 described unlawful conduct are in its possession, custody, and control, to the exclusion of Plaintiff,
28 and await further discovery. When this material information was first revealed to Plaintiff, they

1 exercised due diligence by investigating the situation, retaining counsel, and pursuing their claims.
 2 Defendant intentionally concealed its above-described wrongful conduct. Should such be necessary,
 3 therefore, all applicable statutes of limitation (if any) are tolled under the doctrine of equitable
 4 estoppel.

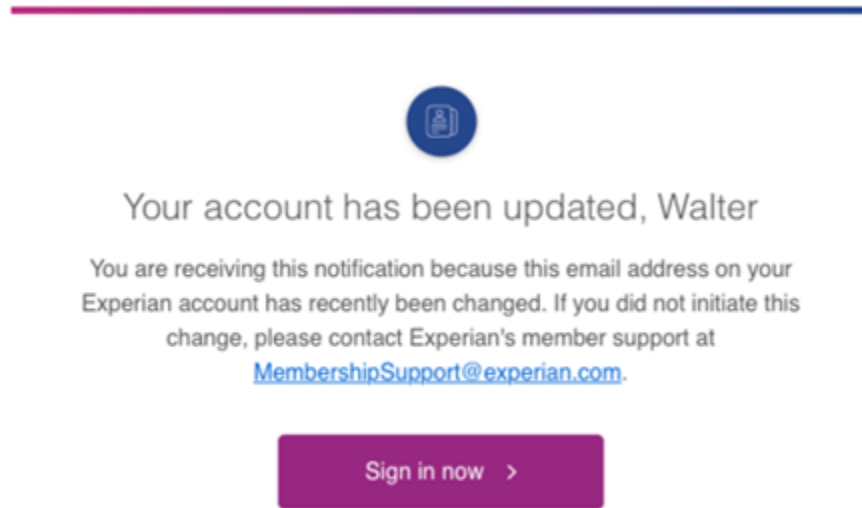
5 106. **EQUITABLE TOLLING.** Defendant took active steps to conceal its above-described
 6 wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the resulting
 7 Security Failure and violations of the FCRA. The details of Defendant's efforts to conceal its above-
 8 described unlawful conduct are in its possession, custody, and control, to the exclusion of Plaintiff,
 9 and await further discovery. When this material information was first revealed to Plaintiff, they
 10 exercised due diligence by investigating the situation, retaining counsel, and pursuing their claims.
 11 Defendant intentionally concealed its above-described wrongful conduct. Should such be necessary,
 12 therefore, all applicable statutes of limitation (if any) are tolled under the doctrine of equitable
 13 tolling

14 **FACTUAL ALLEGATIONS REGARDING THE NAMED PLAINTIFF**

15 107. Plaintiff Walter Hopgood is an adult domiciled in Oregon and has an active Experian
 16 account and had an active account during the entire Class Period.

17 108. Plaintiff Hopgood's experience is demonstrative of the experience of the thousands
 18 of other Class Members who have suffered (1) actual harm resulting from Experian's violation
 19 of the FCRA provisions meant to ensure accuracy, confidentiality, and security of their credit
 20 reports, Consumer Data, and PII, (2) suffered identity theft as a result of the Security Failure
 21 and (3) suffered actual harm as a result of Experian's UCL violations described herein.
 22
 23
 24
 25
 26
 27
 28

109. On the morning of April 21, 2022, Plaintiff Hopgood awoke to an email from Experian saying that the email address from his Experian account had changed.



110. Because Plaintiff had not changed his email address and was unable to log into his Experian account, Plaintiff unsuccessfully attempted to contact a support agent via telephone.

111. At that time, Plaintiff sent an email to, membershipsupport@experian.com. The email read, in part: "I got a message that my email address changed, but I haven't updated it. What's going on? Please advise."

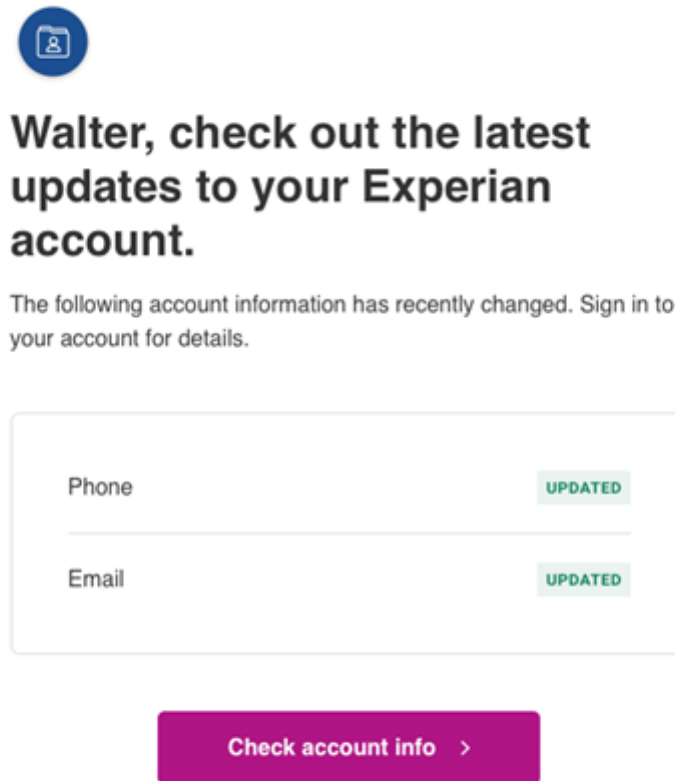
112. After not receiving a response from Defendant, Plaintiff navigated to Experian's website, clicked "Sign up for free" and registered for a new account, using his Social Security number, email address, and phone number.

113. Experian's website stated that Plaintiff had an existing account. Experian's website prompted Plaintiff to answer "generic" knowledge based questions to prove his identity.⁴⁸ For example, "What street have you lived on?" and "What is your mother's maiden name?". Plaintiff observed that the answers to these questions were all publicly available via the internet.

⁴⁸ These "knowledge-based authentication" questions or KBAs are discussed, *supra*.

114. After answering the questions, Plaintiff's access to his Experian account was restored. At that point, Plaintiff received another email from Experian indicating his account email had been changed, indicating that his attempt to restore his account had been successful.

115. The email is screenshotted, below:



116. On the afternoon of April 21, 2022, Plaintiff received an email from Experian alerting Plaintiff that his credit file had been updated with a new credit entry. Upon information and belief, that alert came pursuant to a fraudulent credit inquiry to PedalCard.com. That email alert also indicated that a new Petal credit card application and account had been opened in his name.

1 117. Upon learning of the fraudulent credit card account inquiry, Plaintiff reached
2 out to the Petal and informed the company of the theft. The Plaintiff received a prompt response
3 from the support team, pictured below:

4 **Jarrett (Petal)**

5 Apr 21, 2022, 7:46 PM EDT

6 Hey Walter,

7 We're sorry to hear that you believe you may be a victim of identity theft—we take your security very seriously and we're
8 here to help.

9 If you haven't already, please send us a report as filed with an appropriate (local, state, federal) law enforcement agency
10 detailing the identity theft either via email to support@petalcard.com or by mailing the documents to:

11 Petal Card Inc.
12 MSC – 166931
13 P.O Box 105168
14 Atlanta, GA 30348-5168

15 We will pass this along to our investigations team as soon as we receive it, and we'll let you know as soon as we have an
16 update.

17 In the meantime, please let us know if you have any other information that may help us in our investigation.

18 Thank you,

19 —

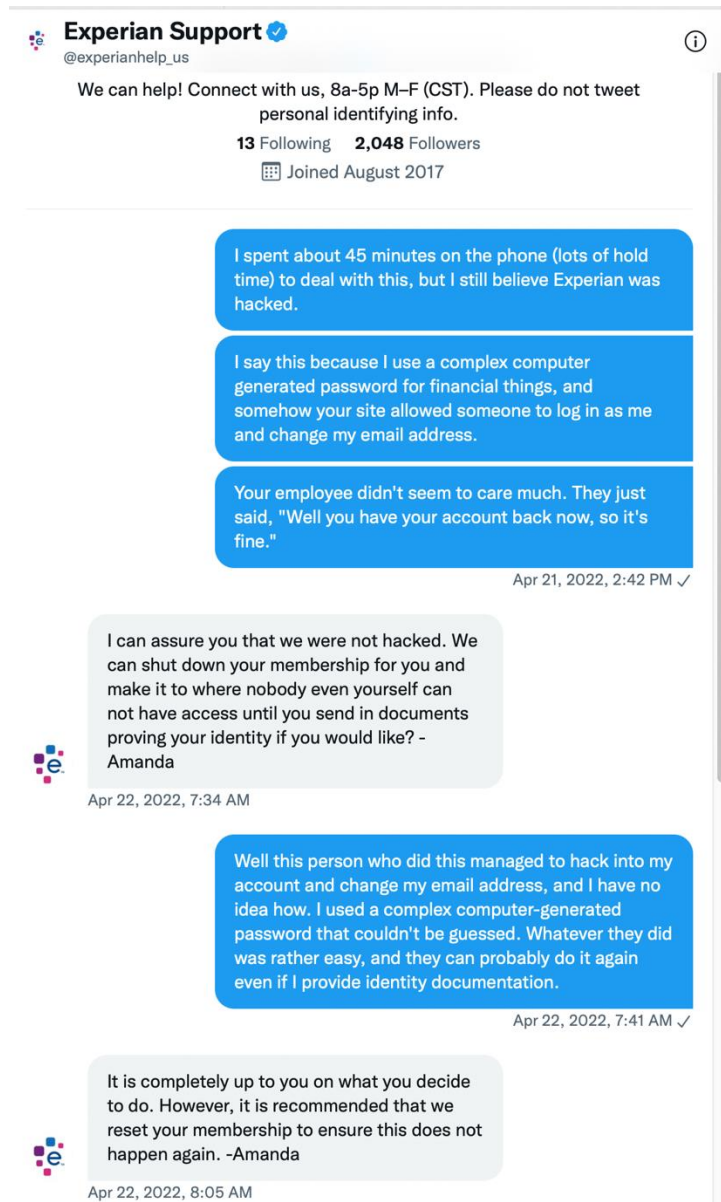
20 **Jarrett - Petal Card**

21 petalcard.com

22 This email is a service from Petal. <https://petalcard.com>

23 118. Plaintiff contacted Clackamas County Sherriff to file a report regarding this
24 identity theft and relayed that information back to Petal.
25
26
27
28

119. Plaintiff again attempted to contact Experian customer support via phone and, after his attempts proved unsuccessful, contacted Experian customer support via Twitter Direct Message. The conversation is detailed below:



120. Plaintiff opened a dispute regarding the PetalCard hard inquiry on April 21, 2022.

121. Plaintiff received an email from Experian on April 21, 2022. The email read, in part, as follows:

We have added an Initial Security to your credit file, which lasts for one year and alerts credit grantors to verify your identity in case someone is using your information without your consent. As an

1 additional precaution, we have removed your name and address
2 from prescreened offer mailing lists for six months.

3 We shared your request with the other CRAs, and you should
4 receive confirmation directly from them. Experian does not accept
5 fraud alert requests submitted by third parties. If you, or your
6 personal representative, placed a fraud alert request directly with
7 one of the other nationwide credit reporting companies, and they
8 refer your request to us, we will honor it to the extent required by
9 the Fair Credit Reporting Act. You can request a free copy of your
10 credit report at 29xperian.com/initialfraudreport or by calling 1 800
11 360 7540. Please retain a copy of this letter.

12 If you write to us, be sure to indicate that you are or feel you may
13 become a victim of identity theft and are requesting your free credit
14 report. Send us copies of the following to Experian P.O. Box 9554
15 Allen, Texas 75013: 1) Your full name including middle initial and
16 generation; 2) Social Security number; 3) complete addresses for the
17 past two years; 4) date of birth; 5) government issued ID card, such
18 as a driver's license, state ID card, etc.; 6) utility bill, bank or
19 insurance statement, etc.

20 122. Later that same day, Plaintiff received an email stating that the dispute had been
21 resolved. Because the hard inquiry from PetalCard had been made at the request of the hacker,
22 Experian removed the credit item from Plaintiff's credit file.

23 123. On or about May 5, 2022, Plaintiff received a letter from First National Bank of
24 Omaha stating that his prequalification inquiry for a credit card with the bank could not be
25 completed due to a credit report lock.

26 124. On the morning of May 6, 2022, Plaintiff again received an email from Experian
27 stating that his email address had been updated, but Plaintiff had not updated his email.

28 125. For the second time in less than a month, the hacker had gained control of Plaintiff's
Experian account. Using this access, the hacker removed the credit lock Plaintiff had placed on the
Experian account.

126. Plaintiff immediately contacted Experian via email on the morning of May
6, 2022. The email read: "For the second time in 3 weeks, someone has hijacked my Experian
account and unlocked my credit. I NEED YOU TO STOP ALLOWING PEOPLE TO DO THIS.
I need to talk to someone but your system will NOT transfer me to a human."

127. After unsuccessfully attempting to contact Defendant via telephone, Plaintiff again reached out to Experian via Twitter Direct Message on May 6, 2022 at 9:06 AM. The conversation is transcribed,⁴⁹ below:

Plaintiff Hopgood (May 6, 2022, 9:06 AM):

Someone just hijacked my Experian account AGAIN.
Someone change my email address to a Hotmail email address without my authorization. I NEED HELP.

Experian Support (May 6, 2022, 9:17 AM):

Hello Walter and thanks for reaching out to us. I understand the concern with this and I'm happy to help. Can you please provide your full name associated with your membership, phone number, and zip code so I can locate your account? Can you also please provide a screenshot of an email that we may have sent you in the past? Thank you. -Maggie

[Plaintiff provided the requested information and screenshot]

Experian Support (May 6, 2022, 9:30 AM):

Thanks for that information and for allowing us to assist you with this matter. This account is being updated so that no one can access it. This may generate another email to be sent to you letting you know that the email address on file has once again been changed.

In order to reinstate the membership, we would need you to send us a copy of the following.

A copy of your driver's license or state- issued ID.
A copy of your social security card
A copy of a recent utility bill, bank statement, or insurance statement.
An explanation of why you are sending this information in.
Include Escalation Ticket: [. . .]

Make sure that the address on your driver's license or state- issued ID matches the utility bill, bank statement, or insurance statement. You would send that to us by fax at 402-458-1634 or by mail at: ECA PO Box 2390 Allen. TX 75013.

Only then can we reset this account. [. . .] Thank you for bringing this to our attention.

⁴⁹ This portion of the exchange is transcribed to protect Plaintiff Hopgood's privacy from further violation.

[. . .]

Plaintiff Hopgood (May 6, 2022, 9:40 AM):

However, I want to stress that this was FAR TOO EASY TO DO. Your site is either hacked, OR the fact that I was able to “create an account” with a different email address and “hack” my account back from whomever hijacked it shows that your site isn’t trustworthy.

Experian Support (May 6, 2022, 9:50 AM):

Thanks, Walter, I do understand the concern with our website. This department will be able to look into your concerns further.

128. Plaintiff sent the requested information via fax to Experian on May 6, 2022. The Plaintiff included the necessary documentation and a letter explaining the situation, yet again, attached as Exhibit 4. The letter stated, in part, as follows:

As I said before, for the second time in two weeks, someone has hijacked my Experian account. They created an email address somewhere (this time it started with "wa" and ended with "hotmail.com") and then went to register an account with Experian. They then went and input my personal details as if they were creating an account and answered the security questions put forth, and moved my email address and change my password. Thankfully your system emailed me at my old email address so that I was notified. They then lifted the credit freeze that I added to my account.

Tell me - what good do your safeguards do if someone can hijack an account this easily?

In order to get my account back - A SECOND TIME - I followed the exact same steps that this fraudulent person did, except with my proper email address. After answering the generic [questions] that most people would be able to answer instead of answering the security questions that I added on my account (which - you know, would be MORE SECURE), I regained access to my account. I changed my security questions and password and contacted your support.

I want to enable 2FA on my account using either [. . .]. Your website touts it, but nowhere have I been able to find it available. And I want it so that NO ONE can just hijack my, or anyone else’s account so damned easily.⁵⁰

⁵⁰ Exhibit 4 (Plaintiff’s Documentation).

1 129. On May 6, 2022 and May 9, 2022, Plaintiff received two identical emails from
2 Experian regarding the situation. The emails read, in part, as follows:

3 This account is being updated so that no one can access it. In order
4 to reinstate the membership, you would need to send us a copies of
5 the following:

6 Your social security card

7 Your state issued id such as a driver's license

8 A utility bill in your name which shows your address
9 matching your license

10 You would send that to us at the following:

11 ECA

12 PO Box 2390

13 Allen. TX 75013

14 You may also fax the information to 402-458-1634.

15 Only then can we reset this account. [. . .] Thank you for bringing
16 this to our attention.

17 130. On May 20, 2022, Plaintiff logged a complaint with the Consumer Financial
18 Protection Bureau because Plaintiff had received no further communication from Experian.

19 131. Plaintiff's understanding was that Experian had revoked his membership on its
20 website, and that he no longer had an Experian account. Since the hacker gained control of his
21 Experian account, Plaintiff has received at least a dozen letters from credit and banking companies
22 regarding fraudulent applications sent by the hacker (e.g. FNBO, Citibank, Discover Card, and
23 AT&T Entertainment) throughout June and July.

24 132. On May 31, 2022, Plaintiff lodged a complaint with the FTC via IdentityTheft.gov.

25 133. Since the hacker first gained control of his Experian account, Plaintiff has received
26 at least a dozen letters from credit and banking companies regarding fraudulent applications sent
27 by the hacker (e.g. FNBO, Citibank, Discover Card, and AT&T Entertainment) throughout June
28 and July. In June, Plaintiff received a phone call from American Express, though he had provided
neither American Express nor Experian with his phone number.

 134. On July 13, 2022, due to the continued application letters Plaintiff received at his
home address, Plaintiff visited Experian's website and attempted to register for an account for
himself.

1 135. Plaintiff discovered that the hacker had, again, created an account in his name
2 without his knowledge following his fax and Experian's repeated assurances that "no one could
3 access" his account following May 6, 2022. The hacker once again provided to Experian false
4 information regarding Walter's email address and home address.

5 136. For a third time, Plaintiff updated his email address, address, and password and
6 regained control of his account. This time, the hacker had changed Plaintiff's home address to an
7 incorrect address.

8 137. Because Plaintiff had unsuccessfully attempted to stop the hacker from taking
9 control of his Experian account three separate times, Plaintiff decided to pay Experian \$25 per
10 month to "freeze" his account for added security using "CreditLock." Using CreditLock, Plaintiff
11 again froze his Experian credit file.

12 138. Using his newly upgraded Experian account, Plaintiff discovered that his Experian
13 Credit Report had been sent to American Express on June 8, 2022, despite Experian's repeated
14 assurances that his account would be safe and despite Experian's knowledge that Plaintiff
15 Hopgood was the victim of identity theft. Plaintiff opened yet another dispute with Experian.⁵¹

16 139. Plaintiff has and will spend considerable time and effort monitoring his accounts to
17 protect himself from identity theft. He fears for his personal financial security and uncertainty over
18 what the hacker may do next. He fears for the security of his information and worries that his
19 property and future are at risk. Plaintiff has and is experiencing feelings of anxiety, sleep
20 disruption, stress, fear, and frustration because of the Security Failure and Experian's disregard for
21 his rights. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort
22 of injury and harm to a consumer that the law contemplates and addresses.

23 140. Plaintiff demands relief on behalf of himself and his similarly situated Class
24 Members

25 **CLASS ACTION ALLEGATIONS**

26 141. Plaintiff seeks relief on behalf of himself and as representative of all others who are
27 _____

28 ⁵¹ The inaccurate credit item and the credit report sent to American Express without a proper purpose are included in Exhibit 5.

1 similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks
 2 certification of a nationwide class defined as follows:

3 **All individuals residing in the United States with Experian**
 4 **consumer accounts associated with their Consumer Data and PII**
 5 **between July 27, 2017 until the Present Date and/or had**
 6 **Consumer Data and PII maintained and collected by Experian**
 7 **within Experian's systems (the "Nationwide Class").**

8 142. Excluded from the Class are the following individuals and/or entities:
 9 Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity
 10 in which Defendant has a controlling interest; all individuals who make a timely election to be
 11 excluded from this proceeding using the correct protocol for opting out; any and all federal,
 12 state or local governments, including but not limited to their departments, agencies, divisions,
 13 bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear
 14 any aspect of this litigation, as well as their immediate family members and staff.

15 143. Plaintiff reserves the right to modify or amend the definition of the proposed
 16 Class before the Court determines whether certification is appropriate.

17 144. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2),
 18 (b)(3) and (c)(4).

19 145. **Ascertainability:** Membership of the Class is defined based on objective
 20 criteria and individual members will be identifiable from Experian's records, including from
 21 Experian's massive data storage, consumer accounts, and enterprise services. Based on
 22 information readily accessible to it, Experian can identify members of the Class who were
 23 victims of Experian's Security Failure and FCRA violations as alleged herein.

24 146. **Numerosity:** Each of the Class consists of thousands of individuals whose
 25 accounts were compromised as a result of the Security Failure and millions of individuals whose
 26 accounts were insecurely maintained as a result of Experian's FCRA violations. Additionally,
 27 millions of individuals experienced actual harm from Experian's willful violation of FCRA in
 28 its refusal to remedy the Security Failure. Accordingly, members of the Class are so numerous
 that joinder of all members is impracticable. Class Members may be identified from

1 Defendant's records, including from Experian's consumer accounts and enterprise services.

2 147. **Predominant Common Questions:** Common questions of law and fact exist
3 as to all members of the Class and predominate over any questions affecting solely individual
4 members of the Classes. Common questions for the Class include, but are not limited to, the
5 following:

- 6 a. Whether, during the class period, Experian disclosed, or adequately disclosed,
7 the Security Failure and/or its insufficient identity verification procedures;
- 8 b. Whether Experian used reasonable procedures to ensure that the information
9 included on consumer credit reports was accurate;
- 10 c. Whether Experian's security insufficiencies, including the Security Failure,
11 violate the FTC Act, the FCRA, or its own Information Policies;
- 12 d. Whether Experian's practice of collecting and utilizing consumer reports and
13 associated Consumer Data and PII violated state and federal laws;
- 14 e. Whether Experian's conduct violates the FCRA;
- 15 f. Whether Experian acted willfully or negligently when allowing the Security
16 Failure to continue without remedy;
- 17 g. Whether Experian has been unjustly enriched by its conduct;
- 18 h. Whether Plaintiff and Class Members are entitled to injunctive relief to enjoin
19 the unlawful conduct alleged herein; and
- 20 i. Whether Plaintiff and Class Members have sustained damages as a result of
21 Experian's conduct and if so, what is the appropriate measure of damages or
22 restitution.

23 148. **Typicality:** Plaintiff's claims are typical of the claims of other Class
24 members, as all members of the Class were uniformly affected by Experian's wrongful conduct
25 in violation of law as complained of herein.

26 149. **Adequacy of Representation:** Plaintiff will fairly and adequately protect the
27 interests of the members of the Class and have retained counsel that is competent and experienced
28 in class action litigation, including nationwide class actions and privacy violations. Plaintiff and

1 their counsel have no interest that is in conflict with, or otherwise antagonistic to the interests
2 of the other Class members. Plaintiff and their counsel are committed to vigorously prosecuting
3 this action on behalf of the members of the Classes, and they have the resources to do so.

4 150. **Superiority:** A class action is superior to all other available methods for the
5 fair and efficient adjudication of this controversy since joinder of all members is impracticable.
6 This proposed class action presents fewer management difficulties than individual litigation and
7 provides the benefits of a single adjudication, economies of scale and comprehensive supervision
8 by a single, able court. Furthermore, as the damages individual Class members have suffered may
9 be relatively small, the expense and burden of individual litigation make it impossible for members
10 of the Class to individually redress the wrongs done to them. There will be no difficulty in
11 management of this action as a class action.

12 151. **California Law Applies to the Entirety of Both Classes:** California's
13 substantive laws apply to every member of the Classes, regardless of where in the United States
14 the Class member resides. Further, California's substantive laws may be constitutionally applied
15 to the claims of Plaintiff and the Class members under the Due Process Clause, *see* U.S. CONST.
16 amend. XIV, § 1, and the Full Faith and Credit Clause, *see* U.S. CONST. art. IV, § 1, of the U.S.
17 Constitution. California has significant contact, or significant aggregation of contacts, to the claims
18 asserted by the Plaintiff and all Class Members, thereby creating state interests that ensure that the
19 choice of California state law is not arbitrary or unfair. Defendant's decision to reside in California
20 and avail itself of California's laws, and to engage in the challenged conduct from and emanating
21 out of California, renders the application of California law to the claims herein constitutionally
22 permissible. The application of California laws to the Class is also appropriate under California's
23 choice of law rules because California has significant contacts to the claims of Plaintiff and the
24 proposed Class and California has the greatest interest in applying its laws here.

25 152. Plaintiff reserves the right to revise the foregoing class allegations and
26 definitions based on facts learned and legal developments following additional investigation,
27 discovery, or otherwise.

28 **COUNTS**

COUNT ONE:
WILLFUL VIOLATIONS OF THE FAIR CREDIT REPORTING ACT
15 U.S.C. § 1681, et seq
(On Behalf of Plaintiff and the Nationwide Class)

153. Plaintiff hereby incorporates Paragraphs 1 through 152 as if fully stated herein.

154. In enacting FCRA, Congress made several findings, including that consumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit information and other consumer information and “[t]here is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer’s right to privacy.” 15 U.S.C. § 1681(a)(4) (emphasis added).

155. Under 15 U.S.C. §1681a(f), a “consumer reporting agency” includes any person which, for monetary fees or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of assembling or evaluating consumer credit information or other consumer information for the purpose of furnishing “consumer reports” to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

156. Experian compiled and maintained a “consumer report” on Plaintiff and Class Members, as defined in 15 U.S.C. § 1681a(d)(1), a “consumer report” is any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used, expected to be used, or collected, in whole or in part, for the purpose of serving as a factor in establishing the consumer’s eligibility for (i) credit or insurance to be used primarily for personal, family, or household purposes, (ii) employment purposes, or (iii) any other purpose authorized by 15 U.S.C. § 1681b.

157. Experian is a national consumer reporting agency as defined in the FCRA. 15 U.S.C. § 1681a(f).

158. As individuals, Plaintiff and Class Members are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

159. As a consumer reporting agency, Defendant was (and continues to be) required to identify, implement, maintain and monitor the proper data security measures, policies,

1 procedures, protocols, and software and hardware systems to safeguard, protect and limit the
 2 dissemination of consumer credit information in its possession, custody and control, including
 3 Plaintiff's and Class Members' credit reports (included associated Consumer Data and PII) only
 4 for permissible purposes under FCRA. *See* 15 U.S.C. 1681(b).

5 160. As a consumer reporting agency, Defendant's actions or inactions that allowed for
 6 the Security Failure also violate its duties and obligations as a credit reporting agency under the
 7 FCRA. Defendant's actions or inactions that allowed for inaccurate credit entries to be included
 8 on Experian consumer credit reports also violate its duties and obligations as a credit reporting
 9 agency under the FCRA. Defendant's conduct when furnishing credit reports to businesses about
 10 the Plaintiff and Class Members when Experian had no reasonable belief that the reports would
 11 be provided for a permissible purpose also violates its duties and obligations under the FCRA.

12 161. As alleged herein, Defendant has engaged in a number of practices that, taken
 13 together, failed to provide reasonable and appropriate security for consumers' personal
 14 information. Among other things, respondent failed to:

- 15 a. Develop and disseminate comprehensive information security policies, including
 16 those related to identity verification for Experian consumer account access and/or
 17 control purposes;
- 18 b. assess the risks of allowing individuals to create Experian credit accounts with
 19 unverified or inadequate identification to access Experian consumer reports
 20 through Experian's website and/or control whether that Experian consumer report
 21 was locked or "frozen" from third-parties;
- 22 c. take appropriate action to correct existing vulnerabilities or threats to personal
 23 information in light of known risks.

24 162. The lack of such security measures directly caused damages to Plaintiff and Class
 25 Members, as detailed herein.

26 163. By its above-described wrongful actions, inaction and omissions, want of ordinary
 27 care, and the resulting Security Failure—to wit, willfully, intentionally, recklessly, negligently,
 28 and knowingly granting access to Experian consumer accounts containing the Consumer Data and

1 PII of millions of U.S. citizens (i.e., the “Class Members”) to any unauthorized individual for
2 several years—Defendant willfully and recklessly violated the FCRA, 15 U.S.C. § 1681, *et seq.*
3 by failing to identify, implement, maintain and monitor the proper data security measures, policies,
4 procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff’s and
5 Class Members’ Experian consumer accounts that contained their Consumer Data and PII.

6 164. As a CRA, Experian may only furnish a consumer report under the limited
7 circumstances set forth in 15 U.S.C. § 1681b, “and no other.” 15 U.S.C. § 1681b(a). None of the
8 purposes listed under section 1681b permit consumer reporting agencies to furnish consumer
9 reports to unauthorized or unknown entities, or computer hackers such as those who accessed
10 Plaintiff’s and Class Members’ Consumer Data, consumer reports, and PII.

11 165. Experian furnished Plaintiff’s and Class Members’ consumer reports, in violation
12 of section 1681b, by disclosing those consumer reports to unauthorized entities and identity
13 thieves, and by allowing unauthorized entities and identity thieves to access their consumer reports

14 166. The FCRA requires Experian, as a consumer reporting agency, to “maintain
15 reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes
16 listed under section 1681b of this title.” 15 U.S.C. § 1681e(a).

17 167. Experian failed to maintain reasonable procedures designed to limit the furnishing
18 of Plaintiff’s and Class Members’ consumer reports to permitted purposes, and/or failed to take
19 adequate security measures that would prevent disclosure of Class Members’ consumer reports to
20 unauthorized entities or computer hackers Defendant has violated 15 U.S.C.A. § 1681e(b)
21 because, due to the Security Failure, Defendant failed to “follow reasonable procedures to assure
22 maximum possible accuracy of the information concerning the individual about whom the report
23 relates.”

24 168. Defendant repeatedly allowed hackers to access Experian consumer accounts and
25 repeatedly created inaccurate credit reports and/or furnished credit reports for impermissible
26 purposes following the inevitable attempts at identity theft that accompanied the hacker’s initial
27 cybercrimes.

28 169. Defendant uses insufficient identifiers in its matching procedures when identifying

1 Experian consumer account holders at the account creation stage and at subsequent credit altering
2 stages of the life of the Experian consumer account.

3 170. In addition to running afoul of the FCRA's accuracy provisions, because Experian
4 uses insufficient identifiers in its matching procedures, Experian improperly relied on its these
5 procedures, which were patently unreasonable, and thus had no reason to believe that all of the
6 information it included its consumer report accurately pertained to the consumer who is the subject
7 of the user's request.

8 171. As alleged in detail herein, Experian's security practices and procedures were so
9 severely deficient or nonexistent, despite its knowledge of the Security Failure and its knowledge
10 that the information contained within Experian's systems and Experian consumer accounts was
11 coveted by attackers and certain to be subject to attempted hacks and exfiltration, that Experian
12 in fact voluntarily and for all practical purposes knowingly offered, provided, and furnished this
13 information to unauthorized third parties.

14 172. As a direct and proximate result of Experian's actions and failures to act described
15 herein, and utter failure to take adequate and reasonable measures to ensure its data systems were
16 protected, Experian offered, provided, and furnished Plaintiff's and Class Members' consumer
17 reports to unauthorized third parties.

18 173. Experian's disclosure of consumer reports under these circumstances was not
19 permitted by, and thus was in violation of, Sections 1681b and 1681e of the FCRA.

20 174. Experian's willful failure to use reasonable matching and/or identity verification
21 procedures resulted in a yet unknown number of inaccuracies on Experian consumer account
22 holder's credit reports, in violation of § 1681e(b), much like the inaccurate inquiry from American
23 Express on Plaintiff Hopgood's Experian credit report.

24 **175.** The credit entry from American Express on Plaintiff Hopgood's Experian credit
25 report was inaccurate because it was both patently incorrect, as it was the result of identity theft,
26 and because it was misleading in such a way that it can be expected to adversely affect future credit
27 decisions. This inaccuracy resulted from Experian's failure to adopt and utilize reasonable
28 procedures to assure maximum possible accuracy of information reported about Plaintiff. Despite

1 the fact that Plaintiff's Experian consumer account had been hacked numerous times, Experian did
2 not require any additional identity verification measures to reopen the account, and continued to
3 provide Plaintiff's credit report in response to businesses seeking to determine Plaintiff's
4 creditworthiness upon the receipt of fraudulent applications.

5 176. Defendant further violated Section 607(a) by furnishing consumer reports though
6 Experian had reasonable grounds for believing that the consumer reports were not going to be used
7 for a permissible purpose (e.g. may be used for fraud).

8 177. In numerous instances, Defendants failed to follow reasonable procedures to assure
9 maximum possible accuracy of their consumer reports. Among other things, Defendants failed to
10 follow reasonable procedures to assure that the information contained in their consumer reports
11 concerned the individual who was the subject of the report.

12 178. FCRA section 604(c) defines when consumer reporting companies may furnish
13 consumer reports in connection with credit and insurance transactions not initiated by the
14 consumer. 15 U.S.C. 1681b(c).

15 179. The statute clearly states that "a consumer reporting agency shall not furnish to any
16 person a record of inquiries in connection with a credit or insurance transaction that is not initiated
17 by the consumer" unless the consumer has given authorization to the consumer reporting agency.
18 15 U.S.C. 1681b(c)(3).

19 180. In numerous instances, Defendants failed to follow reasonable procedures to assure
20 maximum possible accuracy of their consumer reports. Among other things, Defendants failed to
21 follow reasonable procedures to assure that the information contained in their consumer reports
22 concerned the individual who was the subject of the report.

23 181. Defendant's above-described wrongful actions, inaction and omissions, and want
24 of ordinary care, in turn, directly and proximately caused the Security Failure which, in turn,
25 directly and proximately resulted in the wrongful dissemination of Plaintiff's and Class Members'
26 credit reports and inaccurate credit entries onto those reports.

27 182. Defendant's above-described wrongful actions, inaction, omissions, and want of
28 ordinary care, and the resulting Security Failure, directly and proximately caused Plaintiff and

1 Class Members to suffer economic damages and other actual injury and harm, and collectively
2 constitute the willful and knowing violation of the FCRA.

3 183. As a direct and proximate result of Experian's actions and failures to act described
4 herein, and its violation of the FCRA, Plaintiff and Class Members have suffered harm and/or face
5 the significant risk of harm suffering such harm in the future, all as described above

6 184. Plaintiff seeks to recover FCRA statutory damages to the fullest extent allowable
7 by law. In addition Plaintiff also seeks injunctive relief requiring Defendant to, *inter alia*, (i)
8 conduct a full-system audit to finally properly verify the identity of each Experian consumer
9 account holder using its "robust identity verification services;" (ii) identify and notify each U.S.
10 citizen whose Experian Consumer Account (a) was accessed and/or claimed by an unauthorized
11 individual, (b) was otherwise subject to the Security Failure, or (c) was otherwise compromised
12 by the Security Failure; (iii) provide a sum of money sufficient to provide quality credit monitoring
13 and substantial identity theft coverage to each such person for each of their respective lifetimes
14 (iv) establish a fund (in an amount to be determined) to which such persons may apply for
15 reimbursement of the time and out-of-pocket expenses they incurred to remediate identity theft
16 and identity fraud (i.e., data breach insurance), from July 27, 2017 forward to the date the above-
17 referenced credit monitoring terminates, (iv) disgorge its gross revenue from transactions,
18 including but not limited to the revenue derived from selling Consumer Data to business clients
19 for applications created by unauthorized individuals involving Plaintiff's and Class Members'
20 Consumer Data and PII, and the earnings on such gross revenue, and (vi) discontinue its above-
21 described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the
22 causes of the Security Failure.

23 185. Plaintiff and Class Members have standing to sue as a result of Experian's
24 violations of federal and state statutes, including the FCRA, as detailed herein. Further, because of
25 Experian's acts and/or omissions, willful disregard and conduct, and want of ordinary care, and
26 the resulting Security Failure, Plaintiff and Class Members have suffered actual injury have
27 suffered (and will continue to suffer) economic damages and other injury and actual harm in the
28 form of, *inter alia*, (i) actual identity theft and identity fraud, causing immense damage to each

individual's credit score, (ii) invasion of privacy, (iii) loss of the intrinsic value of their privacy, (iv) breach of the confidentiality of their Consumer Data and PII, (v) deprivation of the value of their Consumer Data and PII, for which there is a well-established national and international market, (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages, and (vii) the imminent, immediate, and continuing increased risk of ongoing identity theft and identity fraud. Plaintiff also have standing to bring this suit because Defendant has yet to remedy the cause of the Security Failure.

186. Under Section 1681 of the FCRA, Experian is liable to Plaintiff and Class members for failing to comply with the requirements that a consumer reporting agency not disclose consumer reports and take measures designed to avoid the unauthorized disclosure of consumer reports. Experian therefore is liable to Plaintiff and Class Members for their actual damages as a result of Experian's failure to comply with the FCRA, as well as costs and reasonable attorneys' fees, in amounts to be proven at trial.

187. In addition, Experian's failure to comply with the foregoing requirements was willful because Experian knew or should have known, but recklessly disregarded, that its identity verification, fraud prevention, and cybersecurity measures were inadequate and unreasonable and additional steps were necessary to protect Experian consumer accounts. The willful and reckless nature of Experian's violations is supported by, among other things, its knowledge that its identity verification procedures fall short of their peer consumer reporting agencies, the documented instances in which Experian was informed of the Security Failure, Experian's numerous other security insufficiencies in the past, and Experian's knowledge of similar identity verification issues that remained unresolved and insufficient.⁵²

188. Experian also acted willfully and knowingly because, as a consumer reporting

⁵² See, e.g., KREBSONSECURITY, *Experian Site Can Give Anyone Your Credit Freeze PIN* (Sept. 2017), available at <https://krebsonsecurity.com/2017/09/experian-site-can-give-anyone-your-credit-freeze-pin/> (last visited Jul. 27, 2022); KREBSONSECURITY, *Experian's Credit Freeze is Still A Joke* (Apr. 2021), available at <https://krebsonsecurity.com/2021/04/experians-credit-freeze-security-is-still-a-joke/>; KREBSONSECURITY, *Experian API Exposed the Credit Scores of Most Americans*, KREBSONSECURITY (Apr. 2021), available at <https://krebsonsecurity.com/2021/04/experian-api-exposed-credit-scores-of-most-americans/>.

1 agency, it knew or should have known about its legal obligations regarding data security and
 2 identity verification procedures under the FCRA. These obligations are well established in the
 3 plain language of the FCRA and in the promulgations of the Federal Trade Commission. See, e.g.,
 4 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16
 5 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E. Experian obtained or had available these and
 6 other substantial written materials that apprised them of their duties under the FCRA. Experian
 7 also was directly informed on more than one occasion of the Security Failure and failed to remedy
 8 the Security Failure. Nonetheless, by its utter failure to meet its acknowledged responsibilities and
 9 known duties regarding the need to adopt adequate data security measures, Experian acted
 10 consciously in depriving Plaintiff and Class members of their rights under the FCRA

11 189. Experian's acts described herein constitute a pattern or practice of knowing
 12 violations, as set forth in Section 621(a)(2)(A) of the FCRA, 15 U.S.C. § 1681s(a)(2)(A). Each
 13 instance in which Experian has failed to comply with Sections 604 or 607 of the FCRA, 15 U.S.C.
 14 §§ 1681b, 1681e, constitutes a separate violation of the FCRA for the purpose of assessing
 15 monetary damages.

16 190. Plaintiff and Class Members also are entitled to recover punitive damages, under
 17 15 U.S.C. § 1681n(a)(2), and their attorneys' fees, litigation expenses, and costs, under 15 U.S.C.
 18 § 1681n(a)(3).

19 **COUNT TWO:**
 20 **NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT**
 21 **15 U.S.C. § 1681, *et seq.***
(On Behalf of Plaintiff and the Nationwide Class)

22 191. Plaintiff hereby incorporates Paragraphs 1 through 152 as if fully stated herein.

23 192. In the alternative, by their above-described wrongful actions, inaction and
 24 omissions, want of ordinary care, and the resulting Security Failure, Defendant negligently or in
 25 a grossly negligent manner violated the FCRA by failing to identify, implement, maintain and
 26 monitor the proper identity verification and data security measures, policies, procedures,
 27 protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class
 28 Members' Experian consumer accounts that contained their Consumer Data and PII and credit

1 reports.

2 193. Defendant's above-described wrongful actions, inaction and omissions, and want
3 of ordinary care, in turn, directly and/or proximately caused the Security Failure which, in turn,
4 directly and proximately resulted in the wrongful use of Plaintiff's and Class Members' Experian
5 consumer accounts and use of Plaintiff's and Class Members' consumer reports with no
6 permissible purpose under FCRA, including the facilitation of identity theft and a yet known
7 number of inaccurate credit entries and hard inquiries.

8 194. It was reasonably foreseeable to Defendant that its failure to identify, implement,
9 maintain and monitor the proper identity verification and data security measures, policies,
10 procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and
11 Class Members' Experian consumer accounts would result in a Security Failure, whereby
12 unauthorized third parties would gain access to Plaintiff's and Class Members' Experian
13 consumer accounts and use the control of those accounts to further fraud and identity theft,
14 thereby compromising the accuracy, confidentiality, and security of Plaintiff's and Class
15 Members' consumer credit reports.

16 195. Defendant's above-described wrongful actions, inaction, omissions, and want of
17 ordinary care, and the resulting Security Failure, directly and proximately caused Plaintiff and
18 Class Members to suffer economic damages and other actual injury and harm, and collectively
19 constitute the negligent violation of FCRA. Had Defendant not engaged in such wrongful actions,
20 inaction, omissions, and want of ordinary care, Plaintiff's and Class Members' would not have
21 suffered these injuries, would have been properly protected by the FCRA, and their Experian
22 consumer accounts would not have been used to commit rampant identity fraud. Plaintiff and
23 Class Members, therefore, are entitled to injunctive relief, and compensation for their economic
24 damages, and other actual injury and harm in the form of, inter alia, (i) the lost intrinsic value of
25 their privacy, (ii) deprivation of the value of their PII, for which there is a well-established
26 national and international market, and (iii) the financial and temporal cost of monitoring their
27 credit, monitoring their financial accounts, and mitigating their damages.

28 196. Plaintiff seeks to recover FCRA statutory damages to the fullest extent allowable

1 by law. In addition Plaintiff also seeks injunctive relief requiring Defendant to, *inter alia*, (i)
 2 conduct a full-system audit to finally properly verify the identity of each Experian consumer
 3 account holder using its “robust identity verification services;” (ii) identify and notify each U.S.
 4 citizen whose Experian Consumer Account (a) was accessed and/or claimed by an unauthorized
 5 individual, (b) was otherwise subject to the Security Failure, or (c) was otherwise compromised
 6 by the Security Failure; (iii) provide a sum of money sufficient to provide quality credit
 7 monitoring and substantial identity theft coverage to each such person for each of their respective
 8 lifetimes (iv) establish a fund (in an amount to be determined) to which such persons may apply
 9 for reimbursement of the time and out-of-pocket expenses they incurred to remediate identity
 10 theft and identity fraud (i.e., data breach insurance), from July 27, 2017 forward to the date the
 11 above-referenced credit monitoring terminates, (iv) disgorge its gross revenue from transactions,
 12 including but not limited to the revenue derived from selling Consumer Data to business clients
 13 for applications created by unauthorized individuals involving Plaintiff’s and Class Members’
 14 Consumer Data and PII, and the earnings on such gross revenue, and (vi) discontinue its above-
 15 described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and the
 16 causes of the Security Failure.

17 197. Plaintiff and Class Members also are entitled to recover their attorneys’ fees,
 18 litigation expenses, and costs, under 15 U.S.C. § 1681o(a)(2).

19
 20 **COUNT THREE:**
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW
CAL. BUS. & PROF. CODE §§ 17200, *et seq.*
(On Behalf of Plaintiff and the Nationwide Class)

22 198. Plaintiff hereby incorporates Paragraphs 1 through 152 as if fully stated herein.

23 199. The UCL prohibits any “unlawful, unfair, or fraudulent business act or practice and
 24 unfair, deceptive, untrue or misleading advertising.” Cal. Bus. & Prof. Code § 17200 (UCL). By
 25 engaging in the practices aforementioned, Experian has violated the UCL.

26 200. Experian’s “unlawful” acts and practices include its violation of the FCRA, Section
 27 5 of FTC Act, violation of the Privacy Shield and Frameworks, and violation of its own posted
 28 Information Policies.

201. Experian's conduct violated the spirit and letter of these laws, which prohibit credit reporting agencies from willfully and/or negligently disregarding consumers' rights.

202. Experian's "unfair" acts and practices include its misrepresentations regarding, and failure to disclose the Security Failure, as described above, and its subsequent exploitation of the Security Failure for profit.

203. Plaintiff and Class members have suffered injury-in-fact, including the loss of money and/or property as a result of Experian's unfair and/or unlawful practices, to wit, the unauthorized disclosure and use of their Consumer Data and PII, along with their consumer credit reports which have value as demonstrated by their use profit generation by Experian. Plaintiff and Class Members have suffered harm as detailed within this Complaint.

204. Further, Experian's actions caused damage to and loss of Plaintiff's and Class Members' property right to control the dissemination and use of their personal information.

205. Experian reaped unjust profits and revenues in violation of the UCL. This includes Experian's profits and revenues from their exploitation of the Security Failure and use of Consumer Data and PII for revenue generative purposes. Plaintiff and the Class seek restitution and disgorgement of these unjust profits and revenues.

**COUNT FOUR:
UNJUST ENRICHMENT
[In the Alternative to Counts 1-3]
(On Behalf of Plaintiff and the Nationwide Class)**

206. Plaintiff hereby incorporates paragraphs 1 through 152 as if fully stated herein.

207. Plaintiff and Class Members have an interest, both equitable and legal, in the Consumer Data and PII, including their credit reports, about them that was conferred upon, collected by, and maintained by Experian. This data was conferred on Experian in most cases by third-parties but in some instances directly by Plaintiff and Class Members themselves.

208. Plaintiff and Class Members conferred a benefit on Experian. Specifically, they provided Experian, knowingly or unknowingly, with their Consumer Data and PII, including their credit reports. In exchange, Plaintiff and Class Members should have received from Experian the protection rightfully afforded to such information by the FCRA and other applicable federal and

1 state consumer protection and privacy laws—such as two-factor authentication, account recovery,
2 and/or account re-authentication services and procedures to ensure accurate credit reporting—and
3 should have been entitled to have Experian use reasonable measures to verify their identities and
4 ensure the accuracy of the information connected to their Experian consumer accounts.

5 209. Experian knew that Plaintiff and Class Members conferred a benefit on Experian
6 and has accepted or retained that benefit. Experian profited from the credit reports, Consumer
7 Data and PII of Plaintiff and Class Members for business purposes, without disclosing to, or
8 receiving authorization from, Plaintiff and Class Members to use that information in the unlawful
9 manners described herein, especially considering Experian’s behavior with respect to its
10 exploitation of the Security Failure.

11 210. Thus, Experian acquired the credit reports, Consumer Data, and PII through
12 inequitable means in that it failed to properly protect the credit reports and Experian consumer
13 accounts that contained the Consumer Data and PII from identity thieves and repeatedly
14 misrepresented that it would do so – to both government regulators and to consumers directly.

15 211. Experian also understood and appreciated that the credit reports, Consumer Data,
16 and PII pertaining to Plaintiff and Class Members was private and confidential and its value
17 depended upon Experian maintaining the privacy and confidentiality of such

18 212. But for Experian’s stated willingness and commitment to maintain its privacy and
19 confidentiality, that data (consumer reports, Customer Data, and PII) would not have been provided
20 or transferred to and entrusted with Experian. Further, if Experian had disclosed that its data
21 security, fraud detection, and identity verification measures were inadequate, Experian would not
22 have been permitted to continue in operation by regulators, its shareholders, and participants in the
23 marketplace.

24 213. Plaintiff and Class members have no adequate remedy at law.

25 214. Under the circumstances, it would be unjust for Experian to be permitted to retain
26 any of the benefits that Plaintiff and Class Members conferred on it.

27 215. Experian should be compelled to disgorge into a common fund or constructive
28 trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received—

specifically all revenue related to the Security Failure and/or the savings it conferred upon itself by inadequately securing Experian consumer accounts and the revenue it generated from continuing to sell Experian consumer accounts' associated Consumer Data and PII and credit reports despite understanding that those accounts were compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court:

- a. Certify this action is a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure;
- b. Appoint Plaintiff to represent the Class;
- c. Appoint undersigned counsel to represent the Class;
- d. Award statutory damages, compensatory damages, and punitive damages where available, to Plaintiff and the Class Members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial, including interest thereon;
- e. Award nominal damages to Plaintiff and the Class Members against Defendant;
- f. Non-restitutionary disgorgement of all of Defendant's profits that were derived, in whole or in part, from Experian's collection and subsequent use of Plaintiff's Personal Information;
- g. Ordering Defendant to disgorge revenues and profits wrongfully obtained;
- h. Award Plaintiff and the Class Members their reasonable costs and expenses incurred in this action, including attorneys' fees and expert fees; and
- i. Grant Plaintiff and the Class Members such further relief as the Court deems appropriate.

JURY TRIAL DEMAND

The Plaintiff demand a trial by jury of all issues so triable.

Date: July 28, 2022

Respectfully Submitted,

/s/

1 MICHAEL F. RAM (SBN 104805)
2 **MORGAN & MORGAN COMPLEX**
3 **LITIGATION GROUP**
4 633 West Fifth Street, Suite 2652, Los Angeles,
5 CA 90071
6 Telephone: (415) 358-6913
7 Facsimile: (415) 418-6293
8 mram@ForThePeople.com

9 JOHN A. YANCHUNIS
10 *(Pro Hac Vice application forthcoming)*
11 PATRICK BARTHLE
12 *(Pro Hac Vice application forthcoming)*
13 **MORGAN & MORGAN COMPLEX**
14 **LITIGATION GROUP**
15 201 N. Franklin Street, 7th Floor
16 Tampa, Florida 33602
17 Telephone: (813) 559-4908
18 Facsimile: (813) 222-4795
19 jyanchunis@forthepeople.com
20 pbarthle@ForThePeople.com
21
22
23
24
25
26
27
28

Attorneys for Plaintiff and the Putative Class